

Migration des boîtes aux lettres de AGS vers Microsoft Office 365



Nino Zedoud-Martel | TSR23

Technicien Systèmes et Réseaux

Promotion 2023-2025

Diffusion limitée au CESI, reproduction interdite

Tuteur entreprise

Cyril LAMY

Responsable Achats, Logistique & SI

Pilote de formation

Yoann MALVAL

Responsable de formation

Fiche de confidentialité *Non-disclosure agreement*

2023 V02

Ce document doit être complété pour tout rapport ou mémoire diffusé à CESI École d'Ingénieurs et contenant des informations sur l'entreprise d'accueil.

Ce document est établi en trois exemplaires : un sera conservé par CESI École d'Ingénieur, un autre par l'entreprise, le troisième devra impérativement être intégré au rapport par l'élève.

This page must be included in any document prepared for evaluation purposes at CESI Graduate School of Engineering and that contains information about a host company.

It is produced in three copies: one for the school's records, one for the company, and one which must be included in the student's report.

TITRE DU DOCUMENT EN FRANCAIS	Migration des boites aux lettres de AGS vers Microsoft Office 365
<i>Title of the document in English</i>	Migrating mailboxes from AGS to Microsoft Office 365
NOM DE L'ETUDIANT <i>Student's Name</i>	Nino Zedoud-Martel
PROGRAMME <i>Program</i>	TECHNICIEN SYSTEMES ET RESEAUX – TSR
ENTREPRISE D'ACCUEIL <i>Host company</i>	ASSOCIATION LA RONCE
TUTEUR D'ENTREPRISE <i>In-company supervisor</i>	Cyril Lamy

FICHE DE CONFIDENTIALITE
NON-DISCLOSURE AGREEMENT

☒ **DIFFUSION LIBRE**
Full disclosure

Les rapports / mémoires sont conservés en archives et ils peuvent être librement consultés. Ils peuvent être utilisés par les destinataires, les études peuvent faire l'objet de publication ...

The documents are kept in the school's archives and can be consulted freely. They can be used by anyone who receives them and the studies they contain can be published...

☒ **DIFFUSION RESTREINTE**
Limited disclosure

Les rapports / mémoires **sont restitués à l'entreprise** à l'issue de la soutenance. Aucune reproduction n'est autorisée. La responsabilité de cette opération est confiée au stagiaire. Les informations communiquées oralement aux membres du jury lors de la soutenance font également l'objet d'une obligation de confidentialité. A ce titre, les membres du jury s'engagent à ne pas divulguer ni utiliser, toute information qu'ils seraient amené à connaître pendant une durée indéterminée.

*The documents **will be returned to the company** at the end of the oral presentation. No copies are allowed. Retrieval of the document is the sole responsibility of the student. The information communicated orally to the members of the assessment board during the oral presentation is also subject to confidentiality. The members of the board therefore commit to not divulging or using any information that may come to their knowledge for an indefinite period of time.*

Dans le cadre de la politique de lutte contre le plagiat, les rapports / mémoires seront susceptibles d'être analysés pour en vérifier les sources et ceci quel que soit le mode de diffusion prévu ci-dessus.

As part of our anti-plagiarism policy, it is likely that reports will be analysed to verify the sources, regardless of the level of confidentiality specified above.

Date: 03/07/2025

Date: 01/07/2025

Date:

L'entreprise / The company

L'étudiant/ The student

L'école / The school



Remerciements



Tout d'abord, je tiens à remercier l'équipe pédagogique du CESI de Rouen ainsi que l'ensemble des formateurs pour leur accompagnement et leurs précieux conseils tout au long de ces deux années de formation.

Un grand merci également à Sylvie Maze, grâce à qui j'ai pu entrer en contact avec l'association La Ronce.

Je tiens également à remercier l'association La Ronce, située à Évreux, pour m'avoir accueilli au sein de sa structure malgré l'absence de permis de conduire à cette période. Sans leur confiance, cette alternance n'aurait pas été possible.



Grâce à eux, j'ai pu mettre en pratique mes compétences, tout en m'enrichissant tant sur le plan professionnel qu'humain.

Merci à Stéphane Lasnier, Directeur Général de l'association qui a pris la décision de mettre un scooter à ma disposition afin d'effectuer mes déplacements professionnels le temps d'obtenir mon permis de conduire.

Je remercie également à Cyril Lamy, mon tuteur durant cette expérience. Sa patience, sa disponibilité et sa confiance ont joué un rôle déterminant dans ma progression. Son accompagnement bienveillant a largement contribué à la réussite de mes missions.

De plus, je remercie Philippe Lemasson, infogérant de l'association pour ses conseils qui ont joué un rôle dans ma progression.

Pour continuer, je remercie Maxime Gauthier, DSI externe depuis peu au sein de l'association pour son accompagnement et son aide quand j'en ai besoin.

Ensuite, je remercie l'ensemble des personnes du siège pour leur accueil.

Enfin, je remercie mes proches pour leur soutien moral tout au long de ces deux années.

Table des matières

Migration des boîtes aux lettres de AGS vers Microsoft Office 365	1
Table des matières	2
Introduction générale	4
Partie 1 : Présentation de l'association	5
I. Historique de l'association La Ronce	5
II. Activités	6
Le site rue Lavoisier	6
Le site rue Buisson Saint Jean	7
Le SAVS/SAMSAH	7
La Résidence d'Accueil	8
III. Chiffres clés	8
Budget	8
Effectifs	9
IV. Situation géographique	10
France	10
Local	10
V. Equipe SI	10
VI. Mes missions	11
Partie 2 : Présentation du projet	12
VII. Etat des lieux	12
VIII. Problématique	13
IX. Solution	14
X. Coûts	15
XI. Contraintes	17
XII. Acteurs	17
XIII. Le déroulement du projet	17
XIV. Mise en place de la solution	20
Préparation de l'environnement	20
Lancement de la migration	24
XV. Problématiques rencontrées	25
XVI. Après la migration	26
Automatisation	26
Sécurité	28

Conclusion générale	30
Sommaire d'annexes	1
Liste des acronymes	7
Glossaire	8

Introduction générale

Durant mon alternance au sein de l'association La Ronce, j'ai eu l'occasion de participer à un projet important pour le système d'information de l'association.

L'objectif de ce projet était de remplacer les anciennes messageries hébergées par le prestataire AGS, qui utilisaient encore des boîtes POP et des systèmes peu pratiques ou dépassés, par une solution plus moderne, plus sécurisée et surtout plus adaptée aux besoins des utilisateurs.

Ce mémoire retrace donc les différentes étapes de cette migration, de l'analyse de l'existant jusqu'à la mise en production.

Je vais vous présenter les outils utilisés, les choix techniques qui ont été faits, les difficultés rencontrées ainsi que les solutions mises en place.

C'est un projet complet qui m'a permis de développer mes compétences et de mieux comprendre comment se déroule un véritable projet SI.

Partie 1 : Présentation de l'association

Source : <https://la-ronce.fr/notre-histoire/>

I. Historique de l'association La Ronce

L'association La Ronce a été créée officiellement le 3 mars 1955 à Evreux dans le département de l'Eure pour offrir un accompagnement éducatif, médical et social adapté à des enfants, des jeunes et des adultes en situation de handicap.

Elle fête alors cette année ses 70 ans au service de ces personnes en difficulté.

Le nom de l'association provient du château de La Ronce, construit au XI^e siècle à Fontaine-sous-Jouy. Le château a été ravagé et rénové à plusieurs reprises jusqu'au XII^e siècle.

Durant la seconde guerre mondiale, le château a été occupé par les Allemands puis par l'armée Américaine à la fin de la guerre.

C'est en 1950 que la CAF* de l'Eure rachète le domaine La Ronce encore endommagé par la seconde guerre mondiale. Le château accueillera alors une école départementale de perfectionnement destinée à 25 enfants. En 1954, l'établissement sera reconnu en tant qu'IMP*.

L'association pour la gestion du centre de La Ronce est créée en 1955. Le nom évoluera ensuite pour devenir l'Association La Ronce comme on la connaît aujourd'hui



Le site de Fontaine-sous-Jouy sera ensuite revendu en 2010 et l'IMP déménagera rue Buisson-Saint-Jean à Evreux pour répondre à des exigences d'accessibilité.

II. Activités

L'association compte aujourd'hui plusieurs établissements et services :

Le site rue Lavoisier

Le site rue Lavoisier, à Evreux, a été construit pour accueillir l'IMPro* « Pierre Redon » à partir de 1967 et inauguré en 1970. Pour accompagner les adolescents dans leur formation professionnelle et leur insertion sociale.

À partir de 1982, il accueille le Centre de Rééducation Auditive (CRA) spécialisé dans l'accompagnement des enfants atteints de troubles auditifs. Aujourd'hui ce service s'appelle le SESSAD* « Catherine Louison ».

En 1985, il s'élargit avec la création du CAMSP* « Les Loupiots » qui suit et accompagne les enfants de 0 à 6 ans qui ont des troubles du développement.

Le site héberge également, à partir de 2001, le siège social ainsi que les services supports (technique, logistique, hygiène, blanchisserie & restauration).



Le site rue Buisson Saint Jean

Le site rue Buisson-Saint-Jean à Evreux, qui accueille l'IMP* « Julie Corallo » depuis 2010 pour accompagner les enfants et adolescents âgés de 6 à 16 ans ayant des troubles psychiques et du spectre de l'autisme directement sur place grâce aux quatre unités de vie.

Depuis 2020, le site accueille également le SESSAD* « Mille Couleurs » qui accompagne les personnes directement dans leur cadre de vie.



Le SAVS/SAMSAH

Le SAVS* et le SAMSAH* rue Charles Corbeau permettent de prolonger le parcours des personnes au-delà de la majorité.

Le SAVS* est créé en 1994 pour accompagner les adultes à domicile pour favoriser l'autonomie et maintenir un lien social.

Le SAMSAH* est créé en 2007, ce service fonctionne en complément du SAVS* et est plus médicalisé, il intervient auprès de personnes souffrant de troubles psychiques ou nécessitant un suivi de soins renforcé.



La Résidence d'Accueil

Crée en 2009 en partenariat avec le nouvel Hôpital de Navarre, ce service s'adresse aux personnes souffrant de troubles psychiques stabilisés, mais trop autonomes pour être en institution, et trop vulnérables pour vivre seules sans accompagnement.

Ce service repose sur la sous-location d'appartements avec un suivi individualisé



III. Chiffres clés

Budget

Le budget global de l'association est autour de 11 millions d'euros.

La majorité des fonds provient des subventions publiques qui proviennent de :

- L'ARS*
- Du conseil départemental de l'Eure
- DDETS*

Cet argent sert à entretenir et garantir un accompagnement de qualité des personnes accompagnées.

Effectifs

L'association compte environ 180 salariés dont des éducateurs spécialisés, des éducateurs techniques, des psychologues, des psychomotriciens, des orthophonistes, des ergothérapeutes, du personnel administratif, des médecins et des agents logistiques (entretien des locaux, hygiène des locaux, hygiène du linge, restauration et transports). C'est grâce à ces personnes que l'association peut garantir un suivi des personnes accompagnées.

IV. Situation géographique



France

L'association est composée de 4 sites situés en Normandie

Local

3 sites sont situés sur Evreux et 1 site aux Andelys

Le siège, l'IMPRO, le SESSAD CI et la CAMSP sont situés 13 rue du Lavoisier

L'IMP est situé 3 rue du Buisson Saint Jean

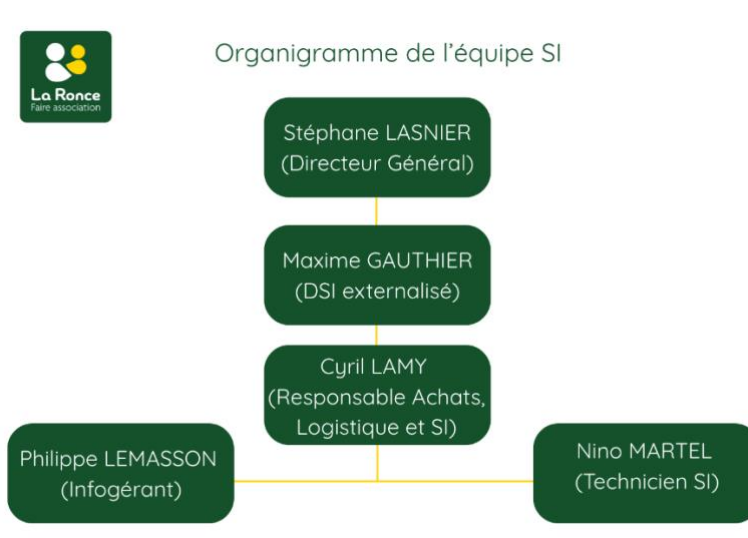
Le SAVS/SAMSAH est situé 23 rue Charles Corbeau

Le CAMSP est également situé 8 Rue des Verriers aux Andelys



V. Equipe SI

L'équipe SI est composée ainsi :



- Stéphane Lasnier (Directeur Général) : Il supervise l'ensemble des activités de l'organisation et prend les décisions stratégiques globales.
- Cyril Lamy (Responsable Achats, Logistique & SI) : Il gère les achats, la logistique et le système d'information, tout en coordonnant les prestataires et techniciens sous sa responsabilité.
- Philippe Lemasson (Infogérant) : Prestataire externe chargé de la gestion courante de l'infrastructure informatique et de l'assistance technique.
- Maxime Gauthier (DSI externalisé) : Responsable de la stratégie informatique de l'association, il accompagne les décisions techniques à un niveau supérieur.
- Nino Martel (Technicien SI) : Technicien interne qui intervient sur les installations, le support utilisateur et la maintenance des systèmes informatiques.

VI. Mes missions

En tant que technicien des systèmes d'information au sein de l'association La Ronce, mes missions consistent à assurer la gestion des tickets d'incidents, diagnostiquer et résoudre les pannes informatiques, ainsi qu'à déployer et remplacer le matériel.

J'interviens aussi bien sur les postes utilisateurs que sur les équipements réseau et les serveurs, garantissant ainsi la continuité et la performance du système d'information.

Partie 2 : Présentation du projet

VII. Etat des lieux

Pour communiquer entre eux les utilisateurs utilisent une messagerie sur un client Outlook et hébergé par AGS. Ce prestataire propose deux services différents de boîtes aux lettres : POP et collaborative.

Les boîtes aux lettres collaboratives utilisent un client Zimbra en IMAP permettant aux utilisateurs d'avoir accès à des fonctions collaboratives avancées comme la possibilité de partager son agenda avec d'autres utilisateurs. Les boîtes aux lettres collaboratives sont également sauvegardées par AGS ce qui permet de ne pas avoir de risque de perte de données.

Initialement ces boîtes étaient destinées aux différents utilisateurs relevant de fonctions administratives et ce pour des raisons économiques.

En revanche les boîtes aux lettres POP ne permettent aucune de ces fonctionnalités. Les mails reçus et envoyés sont uniquement stockés en local sur la machine. Ce qui représente un risque élevé de perte de données en cas de panne.

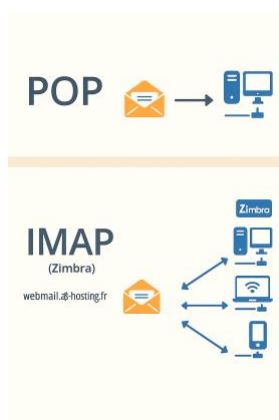


Image générée par IA

Les boîtes aux lettres POP relèvent d'un ancien système qui a ses limites. Les mails sont envoyés du serveur jusqu'au destinataire, une fois le mail reçu il est supprimé du serveur et se retrouve donc uniquement accessible depuis le client de messagerie du destinataire.

En revanche, les boîtes aux lettres IMAP relèvent d'un système plus moderne qui permet la synchronisation entre tous les appareils car le client et le serveur communiquent de façon bidirectionnelle contrairement aux boîtes aux lettres POP.

Les boîtes aux lettres sont réparties de cette façon :

- 64 boîtes en mode collaboratives pour les usages administratifs
- 121 boîtes en mode POP pour les usages éducatifs, médicaux, et paramédicaux

VIII. Problématique

Les boîtes aux lettres hébergées par AGS présentent plusieurs problématiques :

- Nécessitent la configuration manuelle de la messagerie sur la session de l'utilisateur
- Boîtes aux lettres POP non sauvegardées
- Boîtes aux lettres POP limitées à 500Mo
- Manquent de fonctionnalités collaboratives disponibles sur les boîtes aux lettres POP
- Nécessitent l'installation supplémentaire d'un client Zimbra

IX. Solution

Face à ces problématiques et dans un contexte associatif, Microsoft, leader sur le marché, propose plusieurs offres avec des tarifs avantageux pour le secteur associatif. Ils proposent des licences Business Basic, Business Standard et Business Premium pour les associations.

	AGS POP	AGS Collaborative	Business Basic	Business Standard	Business Premium
Travail d'équipe et communication	✗	✗	✓	✓	✓
Version web et mobiles de apps M365	✗	✗	✓	✓	✓
E-mails et calendrier	E-mails uniquement	✓	✓	✓	✓
Stockage et partage de fichiers	✗	✗	✓	✓	✓
Sécurité et conformité	✗	✗	✓	✓	✓
Support et déploiement	✗	✗	✓	✓	✓
Outils pour développer et gérer l'activité	✗	✗	✓	✓	✓
Applications de bureau	✗	✗	✗	✓	✓
Gestion des PC et téléphones	✗	✗	✗	✗	✓
Assistant IA	✗				✓
Protection contre les cyberattaques	✗	✗	✗	✗	✓

Source utilisée : [Comparez les offres Microsoft 365 pour les associations | Microsoft 365](#)

Notre prestataire Philippe Lemasson, nous a recommandé la société Air Cloud qui est spécialisée dans le déploiement de cette solution et certifiée Microsoft.

Après une première réunion exploratoire d'Air Cloud le 2 juin 2024, la solution Microsoft 365 a été retenue en nous proposant 2 prestations.

Pack Modern Workplace :

- Incluant la mise en place de l'infrastructure Microsoft 365
- Incluant un accompagnement clé en main : migration, sécurisation, automatisation
- Incluant un support en illimité
- Incluant des modules de formation en autonomie ou avec un professeur

Pack DSI :

- Pour une infrastructure M365 déjà en place
- Pour former et accompagner l'équipe IT
- Pour une gestion fine et autonome
- Pour des modules de formation en autonomie uniquement

Nous avons donc décidé de prendre le Pack Modern Workplace dans un premier temps afin de réaliser la migration dans les meilleures conditions et d'être accompagné tout au long du processus puis une fois la migration terminée, partir sur le Pack DSI.

X. Coûts

J'ai donc réalisé un comparatif des tarifications actuelles chez AGS et de prévision avec Microsoft Office 365 tout en prenant en compte la prestation d'Air Cloud sur la première année :

Comparatif du cout d'AGS et Microsoft Office 365									
AGS				Office 365					
Type	Prix TTC	Quantité	Cout TTC	Type	Prix HT	Prix TTC	Quantité	Cout TTC	
Boîtes POP	2,89 €	121	349,69 €	Business Premium	5,10 €	6,12 €	15	91,80 €	
Boîtes Collaboratives	5,76 €	64	368,64 €	Business Premium	0 €	0,00 €	20	0,00 €	
				F3	1,87 €	2,24 €	170	381,48 €	
Cout total /mois			718,33 €	Complements					
Cout total /an			8 619,96 €	Sauvegarde	2,20 €	2,64 €	35	92,40 €	
				Services					
				Pack Modern Worksp	595 €	714,00 €	3	2 142,00 €	
				Pack DSI	149 €	178,80 €	9	1 609,20 €	
				Cout total /mois (Pack Modern Workspace)				1 279,68 €	
				Cout total /mois (Pack DSI)				744,48 €	
				Cout total /an (1er année) (3 mois pack Modern Workspace + 9 mois pack DSI)				10 539,36 €	
				Cout total /an (12 mois pack DSI)				8 933,76 €	

Sur les conseils d'Air Cloud nous avons opté pour des licences Business Premium pour le personnel administratif et médical ainsi que des licences Business Basic + F3 pour le personnel technique & éducatif.

Pourquoi cumuler deux licences par utilisateur ?

Car ce sont deux licences complémentaires. Les licences F3 possèdent toutes les fonctionnalités dont les utilisateurs ont besoin mais à une capacité maximale de 2Go pour la messagerie.

Rajouter une licence Business Basic va donc permettre d'avoir 50Go de messagerie gratuitement car en tant qu'association les licences Business Basic sont gratuites jusqu'à 300 utilisateurs.

Il a également été initialement prévu de souscrire au Pack Modern Workplace durant les 3 premiers mois puis le Pack DSI une fois la migration finalisée. A l'heure actuelle le choix a été fait de poursuivre avec le pack Modern Workplace pour continuer de bénéficier de ses avantages.

À la suite de cette analyse, on peut remarquer que le coût d'une telle migration ne sera pas forcément beaucoup plus cher sachant qu'elle permettra d'avoir accès à beaucoup plus de fonctionnalités ainsi qu'à des modules de formation.

XI. Contraintes

Plusieurs contraintes ont été établies :

- Assurer une continuité de service des boîtes aux lettres
- Assurer l'intégrité des données transférés
- Intégration des postes dans l'Active Directory
- Migration des données des boîtes mail POP impossible

XII. Acteurs

Les principaux acteurs de ce projet sont les suivants :

- Stéphane Lasnier (Directeur Général de l'association) : Partie validation du projet et budgétaire
- Cyril Lamy (Responsable Achats, Logistique & S.I) & Maxime Gauthier (Directeur des systèmes d'information externalisé) : Pour la partie supervision du projet
- Philippe Lemasson (Infogérant – Phoenix Informatique) : Pour la partie conseil
- Nino Martel (Technicien systèmes et réseaux) : Pour la partie technique
- Air Cloud : Pour la partie assistance technique et migrations des BAL collaboratives

XIII. Le déroulement du projet

Le projet a débuté au début de l'année 2024, avec une réflexion autour d'une éventuelle migration vers Microsoft Office 365.

En juillet 2024, nous avons rencontré la société Air Cloud afin d'évaluer la faisabilité de cette migration. En parallèle, nous étions à la recherche d'un DSI externalisé dans le but de renforcer les compétences techniques de l'association. Ce besoin a temporairement mis le projet en pause.



Le 7 novembre, j'ai présenté un comparatif prévisionnel des coûts liés à la solution Microsoft.

Le 15 novembre, une réunion de lancement du projet a été organisée avec Air Cloud pour planifier le déploiement de la solution et définir les rôles de chacun.

	Nom	Attribuée à	Début	Fin
1	Lancement de projet		15/11/2024	15/11/2024
2	Préparer et animer la réunion de lancement		15/11/2024	15/11/2024
3	Valider le calendrier prévisionnel		15/11/2024	15/11/2024
4	Azure AD		25/11/2024	25/11/2024
5	Mise en place de l'AD Connect (hors projet)		25/11/2024	25/11/2024
6	Mise en place de MFA		25/11/2024	25/11/2024
7	Création des groupes de sécurité		25/11/2024	25/11/2024
8	Définition de la politique de mot de passe		25/11/2024	25/11/2024
9	Accès conditionnels		25/11/2024	25/11/2024
10	Mise en place SSO (hors projet)		25/11/2024	25/11/2024
11	Migration emails		11/12/2024	27/1/2025
12	Pré-Audit et Audit		11/12/2024	11/12/2024
13	Sécurisation des boîtes aux lettres		11/12/2024	11/12/2024
14	Préparation des DNS et création des users / groupes		24/1/2025	24/1/2025
15	Bascule des DNS		24/1/2025	24/1/2025
16	Migration des emails zimbra vers O365		24/1/2025	24/1/2025
17	Validation de la migration		27/1/2025	27/1/2025
18	Formation utilisateurs (hors projet)		27/1/2025	27/1/2025
19	OneDrive, Sharepoint et Teams		30/1/2025	28/3/2025
20	Audit documentaire		30/1/2025	30/1/2025
21	Création des espaces documentaires (à définir post audit)		30/1/2025	30/1/2025
22	Migration des documents (a définir post audit)		30/1/2025	30/1/2025
23	Validation de la migration (à définir post audit)		28/3/2025	28/3/2025
24	Sécurisation des documents sensibles (labélisation documentaire) à définir post audit		30/1/2025	30/1/2025
25	Formation utilisateurs		30/1/2025	3/2/2025

Le calendrier s'est allongé dans le temps au vu des disponibilités de chacun mais aussi en raison de la fermeture du siège sur les périodes de vacances scolaires. Il s'est donc déroulé comme ceci :

Mise en place

25/11 – Mise en place AD Connect

- Synchronisation de l'Active Directory local avec Azure AD via l'outil Azure AD Connect. Permet une gestion centralisée des identités.

04/12 – Hybridation

- Mise en place d'une architecture hybride pour permettre la coexistence entre les services locaux et Microsoft 365 durant la phase de transition.

Migration de la messagerie

05/12 – Audit mails

- Analyse des boîtes aux lettres existantes, volume de données, et identification des boîtes prioritaires. Permet d'anticiper les problèmes avant migration.

11/12 – Gestion des boîtes aux lettres POP

- Identification et traitement des comptes en POP (protocole non compatible avec Microsoft 365). Conversion en IMAP ou migration manuelle recommandée.

Gestion des identités et droits

05/12 – Entra Connect

- Vérification et configuration d'Entra ID (anciennement Azure AD) pour la gestion des accès et l'authentification.

06/12 – Relancer Entra

- Actions correctives après les premiers tests car problème de synchronisation

07/01 – Réflexion Intune

- Début de l'étude sur la gestion des postes via Intune, pour sécuriser et déployer les politiques sur les appareils.

Automatisation & Sécurité des identités

20/01 – Présentation IA + Entra Connect

- Présentation des solutions IA et de la sécurisation des identités avec :
- Entra Connect + Vérification des comptes
- Harmonisation des noms/préfixes
- Politique d'identités propres à l'organisation

Renforcement sécurité & conformité

04/02 – MFA Fido2

- Mise en place d'une authentification forte (sans mot de passe) via une clé de sécurité Fido2 en essai avec deux utilisateurs.

24/02 – Sécurité - PC Nino

- Enrôlement hybride : Ajout du PC dans Entra ID et Intune.
- MAJ WIN11 : Passage de Windows 10 à 11.
- Analyse Microsoft Defender : Déploiement de Microsoft Defender for Endpoint.

18/03 – Sécurité

- Vérification de l'enrôlement : Contrôle que tous les postes sont bien gérés par Intune.
- Conformité des PC : Application des stratégies (BitLocker, antivirus, MAJ auto...).

24/04 – Sécurité

- Uniformisation de la sécurité sur les postes :
- Réactivation BitLocker
- Application des politiques Intune

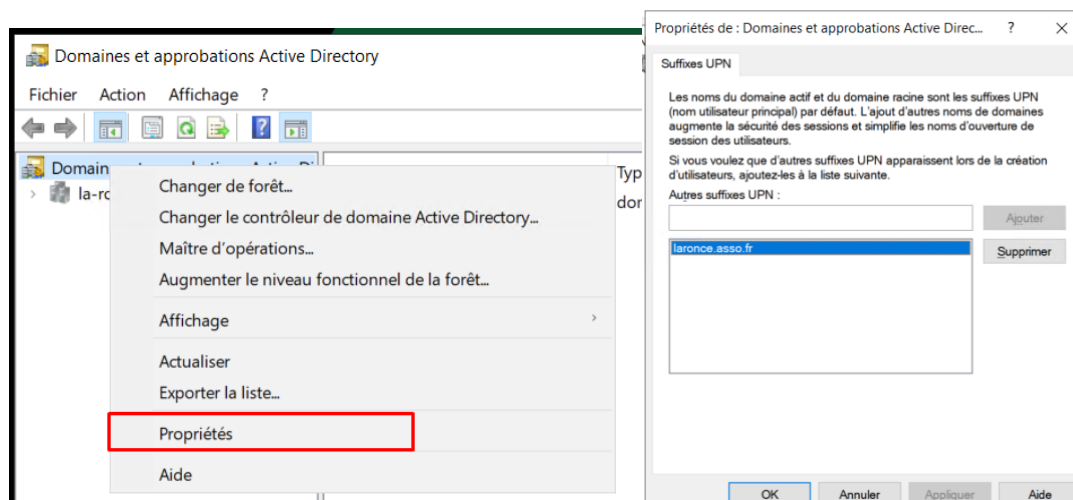
20/05 – Sécurité

- Vérification finale de conformité.
- Activation de Microsoft Defender XDR pour la détection et la réponse étendue aux menaces (toujours en cours).

XIV. Mise en place de la solution

Préparation de l'environnement

Tout d'abord j'ai créé un nouveau suffixe UPN* "laronce.asso.fr" pour permettre et assurer la synchronisation avec l'Azure AD. [Annexe n1](#)



Une fois le nouveau suffixe UPN* créé, j'ai modifié les propriétés de chaque utilisateur afin de leur attribuer le nouveau suffixe UPN*.

Propriétés de : Nino Martel

Membre de	Réplication de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	Contrôle à distance		
Profil des services Bureau à distance		COM+	Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones
		Organisation	Certificats publiés	

Nom d'ouverture de session de l'utilisateur :

N.MARTEL

Nom d'ouverture de session de l'utilisateur (a) :

LA-RONCE\

Horaires d'accès...

Se connecter à...

☒ Déverrouiller le compte

Pour m'éviter de répéter cette action cent-quatre-vingt fois, j'ai utilisé PowerShell afin d'automatiser cette action.

Le script PowerShell que j'ai créé permet de :

- Analyser le suffixe de UPN de l'ensemble des utilisateurs contenus dans l'OU* "Utilisateurs"
- Remplacer le suffixe "la-ronce.local" par "laronce.asso.fr"

Ensuite j'ai ajouté une "proxyAddresses" pour chaque utilisateur afin de lier l'utilisateur à sa messagerie Exchange. [Annexe n1](#)

Propriétés de : Nino Martel

Membre de	Réplication de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	Contrôle à distance		
Général	Adresse	Compte	Profil	Téléphones
Profil des services Bureau à distance		COM+	Éditeur d'attributs	

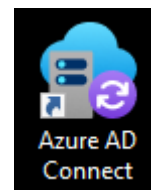
Attributs :

Attribut	Valeur
proxyObjectName	<non défini>
proxyAddresses	SMTP:n.martel@laronce.asso.fr
pwdLastSet	16/10/2023 14:52:18 Paris, Madrid
registeredAddress	<non défini>
repIDProperty/MetaData	AttID Ver Loc.USN Org.DSA
repIDUpToDateVector	<non défini>
repsFrom	<non défini>
repsTo	<non défini>
revision	<non défini>
rid	<non défini>
roomNumber	<non défini>

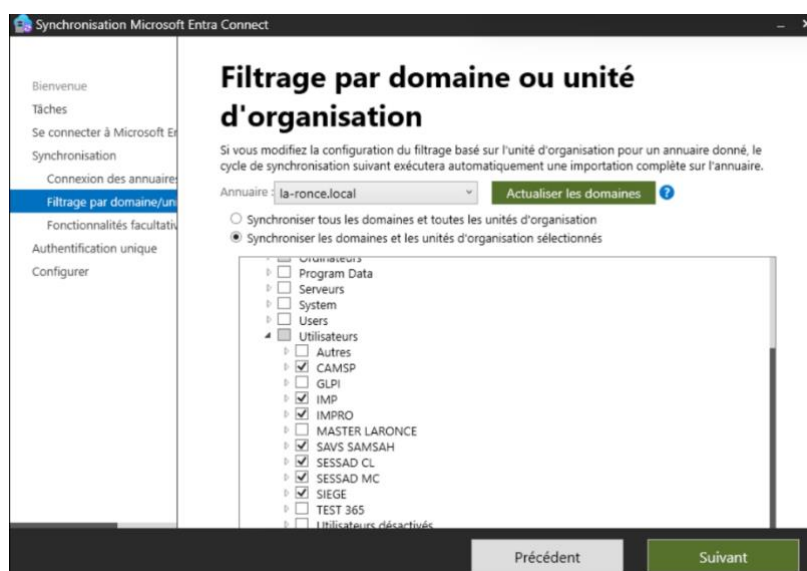
Pour réaliser cette action, j'ai également utilisé un script PowerShell qui :

- Récupère tous les utilisateurs contenus dans l'OU* "Utilisateurs" avec leur UPN* ainsi que leur "proxyAddresses"
- Vérifie que l'utilisateur a bien une adresse email
- Vérifie si les "proxyAddresses" sont vides ou s'il n'y a pas déjà "SMTP:(email)"
- Ajoute "SMTP:(email)" dans les "proxyAddresses"

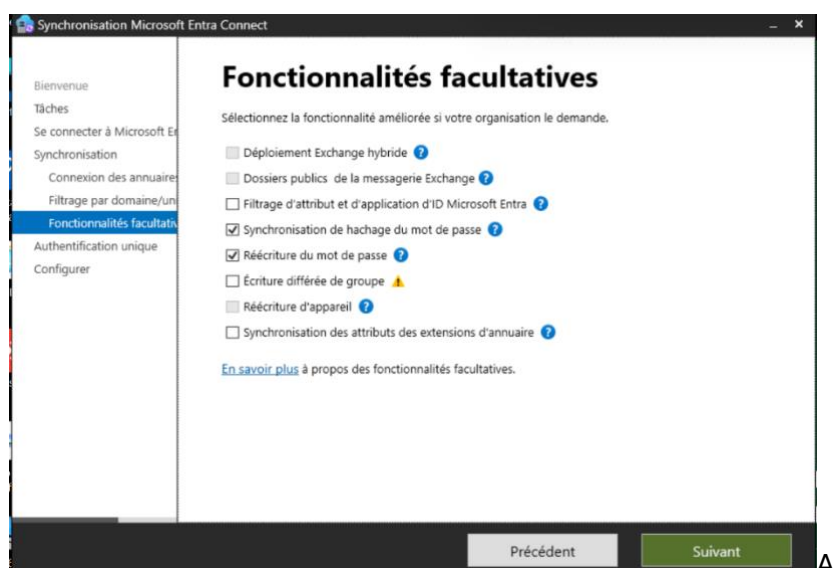
Ensuite j'ai installé Azure AD Connect afin de pouvoir effectuer la synchronisation des utilisateurs de l'AD sur l'Azure AD



J'ai synchronisé l'OU de chaque service afin qu'aucun utilisateur ne soit épargné par la synchronisation



J'ai ensuite synchronisé le mot de passe des utilisateurs afin que les utilisateurs aient un mot de passe unique



Par défaut, la synchronisation de l'AD Connect s'effectue toutes les 30 minutes. J'ai donc forcé la synchronisation à l'aide de cette commande PowerShell :

```
Start-ADSyncSyncCycle -PolicyType Delta
```

J'ai ensuite vérifié que la synchronisation s'est bien effectuée sur le centre d'administration Microsoft 365

☐ Nom d'affichage ↑	Nom d'utilisateur	Licences	État de syn...	Choisissez les colonnes
☐ Nino Martel	N.MARTEL@laronce.asso.fr	Microsoft Power Automate Free , Don de Microsoft 365 Business Premium		Synchronisé à partir d'une instance locale

Afin de renforcer la sécurité, j'ai déployé une GPO* pour définir une politique de mot de passe stricte de 14 caractères et devant respecter des exigences de complexité telle que : des majuscules, minuscules, chiffres et caractères spéciaux. Les mots de passe ne peuvent également pas contenir le nom ou le prénom de l'utilisateur.

Configuration ordinateur (activée)		masquer
Stratégies		masquer
Paramètres Windows		masquer
Paramètres de sécurité		masquer
Stratégies de comptes/ Stratégie de mot de passe		masquer
Stratégie	Paramètre	
Antériorité maximale du mot de passe	0 jours	
Antériorité minimale du mot de passe	0 jours	
Appliquer l'historique des mots de passe	0 mots de passe mémorisés	
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé	
Le mot de passe doit respecter des exigences de complexité	Activé	
Longueur minimale du mot de passe	14 caractères	

J'ai déployé une seconde GPO* pour mettre en place des raccourcis vers Outlook web afin de faciliter l'accès à la messagerie pour les utilisateurs durant la migration

Éditeur de gestion des stratégies de groupe					
Fichier Action Affichage ?					
Stratégie Raccourci_Webmail [S] Configuration ordinateur Stratégies Préférences Configuration utilisateur Stratégies Paramètres du logici Paramètres Windows Modèles d'administr Préférences Paramètres Windows Applications Mappages de lec Environnement Fichiers Dossiers Fichiers.ini Registre Raccourcis Paramètres du Pann					
Raccourcis Traitement en cours Nom Ordre Action Raccourci Cible					
Messagerie Outlook 1 1 Mettre ... %DesktopDir%\Messagerie Outlook https://outlook.office.com/mail/ Messagerie Outlook 2 2 Mettre ... %StartMenuDir%\Messagerie Out... https://outlook.office.com/mail/ Messagerie Outlook 3 3 Mettre ... %RecentDocumentsDir%\Messag... https://outlook.office.com/mail/ Messagerie Outlook 4 4 Mettre ... %FavoritesDir%\Messagerie Outlo... https://outlook.office.com/mail/					
Description Aucune stratégie sélectionnée					
Préférences Étendu Standard					

Enfin j'ai modifié les entrées DNS hébergées par Orange Business afin que les boîtes aux lettres Microsoft 365 soient fonctionnelles

Type	Nom	TTL	Valeurs	Actions
NS	laronce.asso.fr	86400	ns01.eolas.fr.	Aucune
NS	laronce.asso.fr	86400	ns02.eolas.fr.	Aucune
NS	laronce.asso.fr	86400	ns03.eolas.fr.	Aucune
MX	laronce.asso.fr	86400	0 laronce-asso-fr.mail.protection.outlook.com.	Aucune
TXT	laronce.asso.fr	86400	"MS=XXXXXXXXXX"	Aucune
TXT	laronce.asso.fr	86400	"MS=XXXXXXXXXXXXXXXXXXXXX"	Aucune
TXT	laronce.asso.fr	86400	"v=spf1 include:spf.cloud.vadesecure.com include:spf.protection.outlook.com -all"	Aucune
TXT	_dmarc.laronce.asso.fr	86400	"v=DMARC1; p=none; pct=100"	Aucune

Lancement de la migration

La migration de l'ensemble des données s'est déroulée durant le week-end du 24 janvier au 27 janvier afin d'impacter le moins d'utilisateurs. Cette migration a donc été supervisée par Air Cloud.

Nous avons adressé un mail en amont à l'ensemble des utilisateurs leur indiquant de ne pas utiliser leur boîte mail ce vendredi 24 janvier afin de ne perdre aucune donnée durant le processus de migration et en leur indiquant également la procédure à suivre à leur retour le lundi matin pour se connecter à leur nouvelle messagerie. [Annexe n3](#)

Dès le lundi matin 27 janvier, l'équipe composée de Philippe Lemasson, Cyril Lamy et moi-même avons été mobilisés pour créer des backups des anciennes boîtes mail POP sur le poste de chacun des utilisateurs afin de pouvoir réimporter les données dans les nouvelles boîtes mail Microsoft Office 365. [Annexe n4](#)

La migration s'est donc finalement terminée avec succès. Cependant, 50 postes n'étaient pas connectés au domaine. Cela veut dire que le compte utilisateur n'est pas directement lié au compte Microsoft. Cela pose donc un problème de sécurité étant donné qu'aucune GPO ne s'appliquent.

J'ai donc dû intégrer au plus vite ces postes dans l'AD local en faisant en sorte de ne pas trop impacter les utilisateurs. Aujourd'hui tous les postes sont intégrés dans l'AD local sur le domaine "la-ronce.local".

Utilisateurs et ordinateurs Active Directory (S/	Nom d'ouverture de session antérieur ...	Nom	Description	Type	Téléphone (bur...	Fonction
Requêtes enregistrées	MP-19002\$	MP-19002		Ordinateur		
la-roncelocal	MP-19003\$	MP-19003		Ordinateur		
Builtin	MP-19004\$	MP-19004		Ordinateur		
Computers	MP-20001\$	MP-20001		Ordinateur		
Domain Controllers	MP-20002\$	MP-20002		Ordinateur		
ForeignSecurityPrincipals	MP-21001\$	MP-21001		Ordinateur		
Groupes de sécurité	MP-21002\$	MP-21002		Ordinateur		
Keys	MP-21003\$	MP-21003		Ordinateur		
LostAndFound	MP-22001\$	MP-22001		Ordinateur		
Managed Service Accounts	MP-22002\$	MP-22002		Ordinateur		
Ordinateurs	MP-22003\$	MP-22003		Ordinateur		
HYBRIDATION365	MP-22004\$	MP-22004		Ordinateur		
Program Data	MP-25001\$	MP-25001		Ordinateur		
Serveurs	MP-25002\$	MP-25002		Ordinateur		
System						

XV. Problématiques rencontrées

J'ai rencontré plusieurs difficultés techniques :

- Pas de migration possible des données des boîtes aux lettres POP

Les salariés disposant d'anciennes boîtes aux lettres POP n'ont pas bénéficié de la migration automatique de leurs données car ce type de boîte mail ne le permettait pas.

L'équipe et moi-même avons donc dû faire l'export des données vers un fichier pst que nous avons ensuite importé dans la nouvelle messagerie Office 365

- Connexion incomplète au domaine local

Lors de la migration, 50 postes n'étaient encore pas connectés au domaine local. Cela représente un problème de sécurité car les GPO de stratégie de mot de passe et raccourci vers ne s'appliquent pas.

De plus les utilisateurs ne connaissaient pas leur mot de passe. On a donc dû en créer et leur distribuer le temps d'effectuer la connexion avec le domaine local.

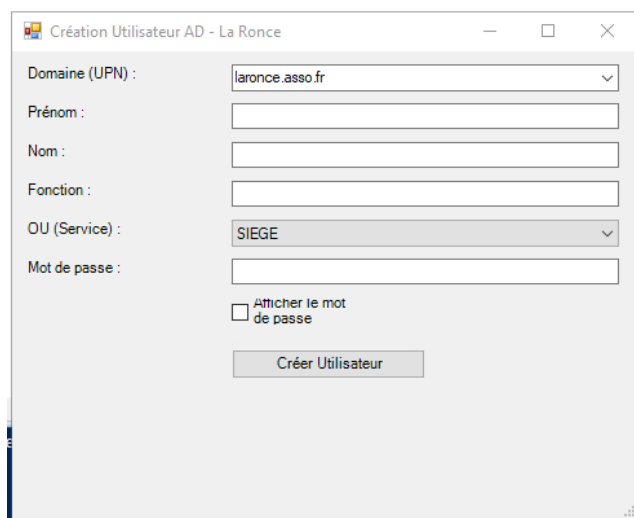
Ces difficultés ont nécessité une mobilisation importante de l'équipe informatique pour assurer la continuité du service.

XVI. Après la migration

Automatisation

Une fois qu'office 365 a été déployé, j'ai mis en place un script PowerShell pour créer les nouveaux utilisateurs de façon automatique afin de ne pas avoir à paramétrer manuellement les propriétés de chaque nouvel arrivant. [Annexe n5](#)

Cela permet donc un gain de temps et empêche l'erreur humaine.



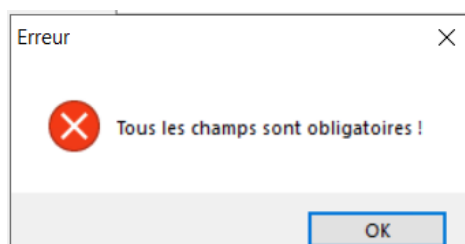
Voici les fonctionnalités de mon script PowerShell :

Interface :

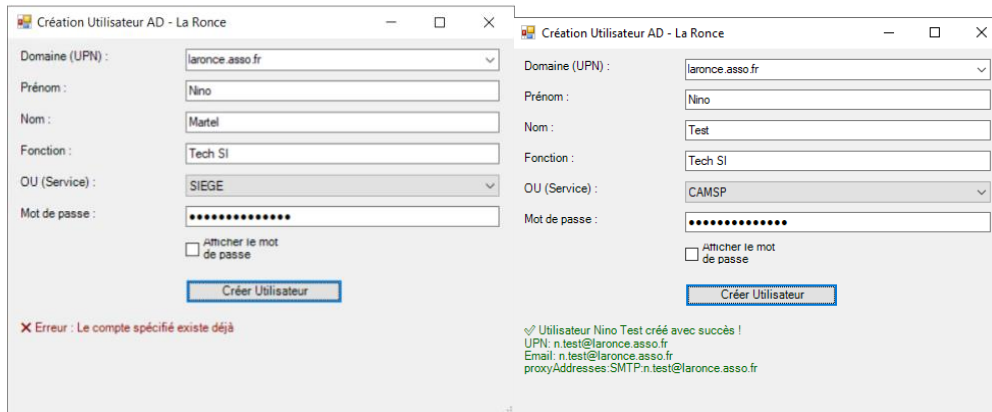
- Menu déroulant pour le choix du suffixe UPN
- Choix du Nom, Prénom & fonction de l'utilisateur
- Menu déroulant pour le choix du service
- Choix du mot de passe avec la possibilité de l'afficher

Bouton "Créer Utilisateur" :

- Affichage d'un message d'erreur si un champ obligatoire est vide



- Création du nom d'utilisateur grâce à la première lettre du prénom, suivie d'un point et du nom, le tout en minuscule.
- Générée à partir du nom d'utilisateur + @laronce.asso.fr
- Application du suffixe UPN choisi
- Détermine l'OU choisi
- Ajout de l'adresse mail dans les "proxyAddresses" : SMTP:(email)
- Force la synchronisation avec Azure AD
- Affiche un message de réussite ou d'échec



The image displays two side-by-side screenshots of a web form titled "Création Utilisateur AD - La Ronce".

Left Screenshot (Error):

- Domaine (UPN): laronce.asso.fr
- Prénom: Nino
- Nom: Martel
- Fonction: Tech SI
- OU (Service): SIEGE
- Mot de passe: [masked]
- ☐ Afficher le mot de passe
- Créer Utilisateur
- Message: **Erreur : Le compte spécifié existe déjà**

Right Screenshot (Success):

- Domaine (UPN): laronce.asso.fr
- Prénom: Nino
- Nom: Test
- Fonction: Tech SI
- OU (Service): CAMSP
- Mot de passe: [masked]
- ☐ Afficher le mot de passe
- Créer Utilisateur
- Message: **Utilisateur Nino Test créé avec succès !**
- UPN: n.test@laronce.asso.fr
- Email: n.test@laronce.asso.fr
- proxyAddresses: SMTP:n.test@laronce.asso.fr

Sécurité

Maintenant que tout est en place, nous avons engagé la partie sécurité avec Air Cloud qui est encore d'actualité.

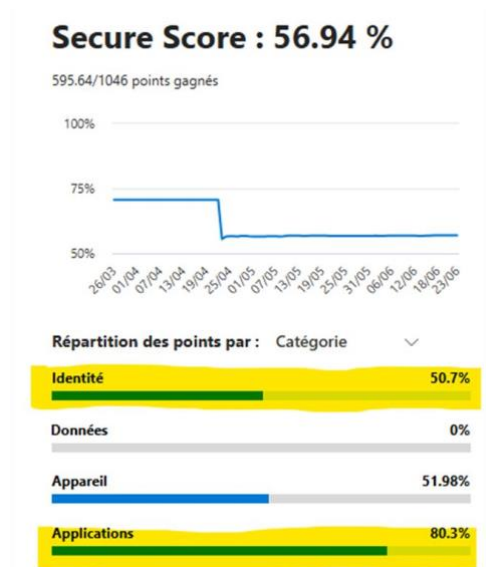
Nous avons donc mis en place :

- La sécurité des identités
- La sécurité des applications
- La synchronisation des utilisateurs entre l'AD et Microsoft Entra avec Entra Connect

Annexe n6

Aujourd'hui nous en sommes à l'étape d'enrôlement hybride des appareils dans Microsoft Entra/Intune

Sur le centre d'administration, un score nous est attribué en fonction de notre niveau de sécurité



Microsoft compare également notre score à celui d'organisations de taille similaire.



Sur la capture, nous avons un score plutôt correct par rapport à d'autres organisations. Cependant il nous reste encore quelques étapes de sécurisation à terminer.

Actuellement nous sommes sur la partie enrôlement des postes dans Intune mais certains postes rencontrent certains problèmes bloquants.

Pour débloquent l'enrôlement j'ai dû accéder aux postes des utilisateurs concernés pour effectuer des manipulations dans le registre ainsi que dans le dossier "Local" des utilisateurs. [*Annexe n7*](#)

Ensuite, il nous reste à activer la double authentification grâce aux clés fido2 pour l'ensemble des utilisateurs ainsi que Microsoft Defender XDR pour la détection étendu aux menaces

L'authentification par clé fido2 permet une double authentification physique, ce qui renforce la sécurité par rapport à une authentification par SMS par exemple.

Quant à Microsoft Defender XDR, c'est une solution de sécurité tout-en-un qui détecte, analyse et répond automatiquement aux menaces sur les postes, les mails, les identités et les applications.

Etant donné que j'effectue ma troisième année à l'association La Ronce, j'aurais donc l'occasion de finaliser ces étapes de sécurité.

Conclusion générale

Ce projet de migration des boîtes aux lettres vers Microsoft Office 365 m'a permis de mettre en pratique mes compétences ainsi que d'appliquer les éléments abordés au cours de ma formation.

Même si certaines étapes ont été compliquées, j'ai toujours trouvé des solutions en m'appuyant sur mes connaissances avec le support le cas échéant de l'équipe SI.

Aujourd'hui, toutes les boîtes aux lettres sont migrées, les utilisateurs peuvent accéder à leurs mails de manière simple et sécurisée, et le système est prêt pour les prochaines évolutions, notamment au niveau de la sécurité.

Ce projet m'a beaucoup appris, autant sur le plan technique que sur le plan humain, et m'a permis de voir concrètement comment un projet peut avoir un véritable impact sur le fonctionnement d'une structure comme La Ronce.

Je suis fier d'avoir pu y participer et je continuerai à accompagner l'association sur ces sujets lors de ma troisième année d'alternance.

Sommaire d'annexes

Annexe n1	1
Annexe n2.....	2
Annexe n3.....	3
Annexe n4.....	4
Annexe n5.....	6
Annexe n6.....	8
Annexe n7.....	10

Annexe n1

Script PowerShell pour remplacer le suffixe UPN de l'ensemble des utilisateurs :

```
upnps1* X
1 $localUsers = Get-ADUser -Filter {UserPrincipalName -like '*la-ronce.local'} -SearchBase "OU=Utilisateurs,DC=la-ronce,DC=local" -SearchScope Subtree -Properties UserPrincipalName -ResultSetSize $null
2
3 $localUsers | ForEach-Object {
4     $newUpn = $_.UserPrincipalName.Replace("la-ronce.local","laronce.asso.fr")
5     $_ | Set-ADUser -UserPrincipalName $newUpn
6 }
7
```

Script PowerShell pour ajouter une proxyAddress sur l'ensemble des utilisateurs :

```
ProxyAddresses.ps1* X
1 $DC = ""
2 $Base = "OU=Utilisateurs,DC=la-ronce,DC=local"
3 $Users = Get-ADUser -Server $DC -SearchBase $Base -SearchScope Subtree -Filter * -Properties UserPrincipalName,proxyAddresses
4
5 foreach ($u in $Users) {
6     $email = $u.UserPrincipalName
7     if (!$email) { continue }
8
9     if (!$u.proxyAddresses -or -not ($u.proxyAddresses -contains "SMTP:$email")) {
10         $proxies = @($u.proxyAddresses) + "SMTP:$email"
11         Set-ADUser -Identity $u -Server $DC -Replace @{proxyAddresses = $proxies}
12     }
13 }
14
```

Annexe n2



📍 Bois-Guillaume
 ☎ 06 51 50 80 76
 ✉ contact@ninomartel.fr
 💻 ninomartel.fr

Formations

2023 - 2025
 Cesi
TSR (Technicien systèmes et réseaux)

2022 - 2023
 Campus La Chataigneraie
**BTS SIO - SISR (Services Informatiques aux
 Organisations option Solutions d'infrastructure,
 systèmes et réseaux)**

2019 - 2022
 Lycée Marcel Sembat
**BAC PRO SN - ARED (Systèmes Numérique option
 Audiovisuels, Réseau et Équipements Domestiques)**

Skills

- Maintenir et dépanner un parc informatique
- Installer, administrer les systèmes Windows & Linux
- Notions de programmation (PowerShell, HTML, LUA)

Hobbies

- Création et gestion de serveurs perso (NAS, Raspberry Pi)
- Cybersécurité
- Bourse / Immobilier
- Musculation
- Automobile / Simulation auto
- VTT
- Assemblage et réparation d'ordinateurs

Nino Martel

Administrateur Systèmes et Réseaux | En alternance à Cesi

Expériences professionnelles

Association La Ronce

Technicien Systèmes et réseaux | Octobre 2023 --> Septembre 2025

- Résolution de pannes matérielles informatiques auprès des utilisateurs
- Mise en place d'un outil de gestion de parc informatique et de suivi des stocks (GLPI)
- Gestion des tickets d'incidents via un système de support
- Support technique aux utilisateurs par assistance téléphonique
- Remplacement et configuration de postes de travail et d'ordinateurs portables

Hôtel de Bourgheroulde

CDD | Juillet 2023 --> Octobre 2023

- Réaménagement des espaces de travail et de stockage
- Préparation des chambres et des lits selon les standards de l'établissement
- Installation de lits supplémentaires et d'équipements pour bébés sur demande
- Maintien de la propreté et de l'accessibilité des couloirs

Promosoft

Stage | Juin 2023

- Support technique auprès des utilisateurs pour la résolution de pannes informatiques
- Gestion et suivi des tickets d'incidents
- Assistance technique par téléphone
- Vérification et mise à jour de la documentation technique
- Rédaction de comptes-rendus d'interventions

CARDIF IARD

Stage | Mai 2021, Novembre 2021 & Mars 2022

- Assistance technique aux utilisateurs pour les pannes matérielles et logicielles
- Gestion des tickets d'incidents via Jira
- Suivi de l'inventaire et gestion des équipements informatiques
- Participation au déploiement et à l'installation de nouveaux équipements

MDA

Stage | Janvier 2021

- Livraison, installation et configuration d'appareils électroménagers
- Gestion du stock et organisation des zones de stockage
- Accueil et conseil client
- Assemblage et montage de mobilier

Prodistrib

Stage | Mars 2020

- Assemblage et démontage d'ordinateurs
- Réparation et maintenance de matériels informatiques
- Installation et configuration de systèmes d'exploitation

Annexe n3

Mail informatif envoyé aux utilisateurs juste avant la migration

Bonjour à tous,

Dans le cadre de l'évolution des outils informatiques mis à disposition de ses collaborateurs, l'Association a opté pour des solutions collaboratives avancées pour tous: Microsoft Office 365. Il s'agit bien d'une évolution et non d'une révolution.

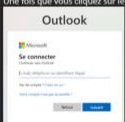
La mise en place de ces outils nécessite une coupure totale des accès mails le Vendredi 24 Janvier 2025.

La consultation des mails et l'envoi de mails (ouverture Outlook sur le PC, consultation via le Webmail, ouverture de l'appil sur les smartphones) à compter de ce vendredi est donc interdite, vous serez donc coupés de cet accès sur cette journée(mais aussi le samedi pour le pôle adultes).

Il convient donc de prendre toutes les dispositions nécessaires en amont pour avoir accès notamment à son agenda, vous pouvez par exemple faire des copies d'écran de votre agenda du vendredi 24/01/25 au lundi 27/01/25 et stocker ces dernières sur votre poste informatique.

A partir de lundi 27/01/25 vous devrez vous connecter à votre boîte mails via le raccourci bureau (Cet icône est déjà présent sur votre bureau il a été déployé ce jour mais cet icône ne vous servira qu'à compter de lundi 27 Janvier 2025)

Une fois que vous cliquez sur le raccourci mentionné, votre navigateur internet va s'ouvrir et cette fenêtre va apparaître :

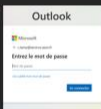


Pour se connecter, renseigner l'adresse de votre boîte mail.

Une seconde fenêtre s'ouvre alors (cf ci-dessous), cliquer sur Compte professionnel ou scolaire :



Une dernière fenêtre s'ouvre alors (cf ci-dessous), il convient alors de renseigner votre mot de passe d'ouverture de session Windows



Certains d'entre vous n'auront pas l'historique des mails (reçus et envoyés), néanmoins en cas de besoin vous pourrez les consulter et juste les consulter via l'ancien accès OUTLOOK. Nous devrons passer individuellement sur les postes afin de les réinjecter, cette opération se fera sur la durée, soyez indulgent.

En cas de problématique lundi matin pour l'ouverture de votre boîte mails, merci de nous appeler ou de nous envoyer un SMS pour les collaborateurs dotés d'un téléphone portable professionnel.

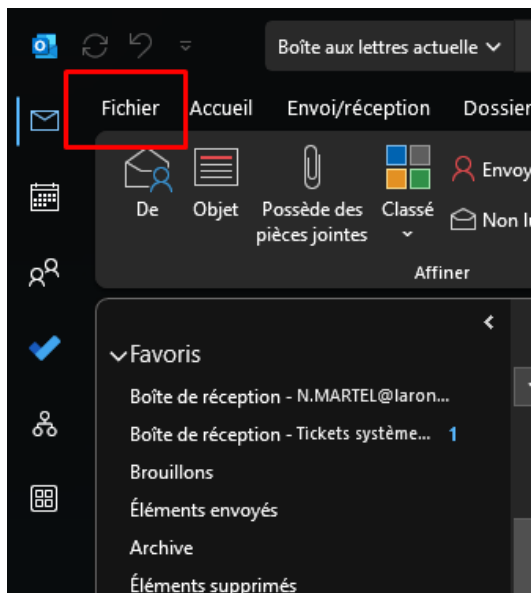
Nous vous remercions par avance pour la bonne prise en compte de ces éléments afin que le déploiement de ces nouvelles solutions se déroulent sereinement.

Très bonne fin de journée

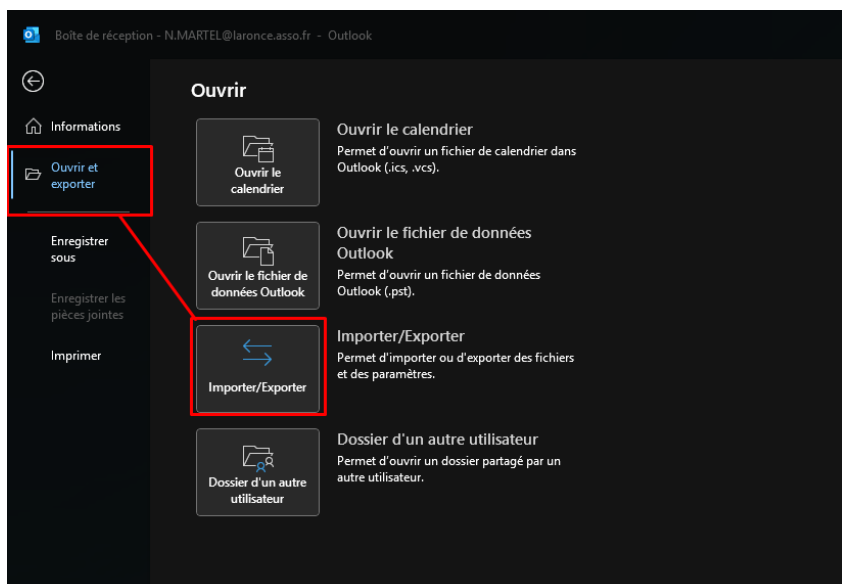
Annexe n4

Procédure de migration des boîtes mails POP :

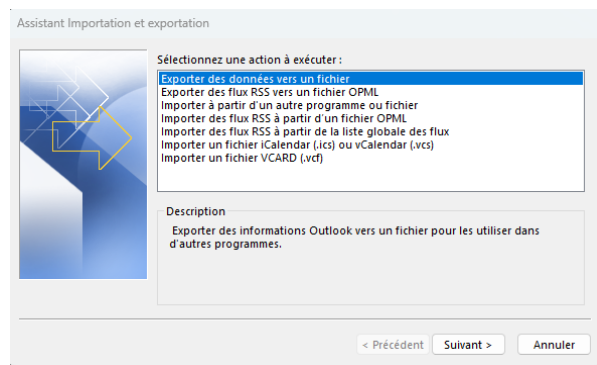
1)



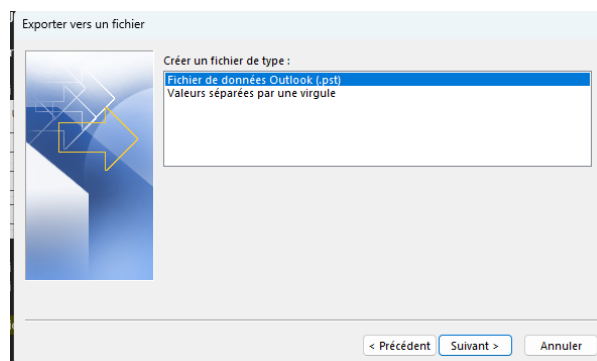
2)



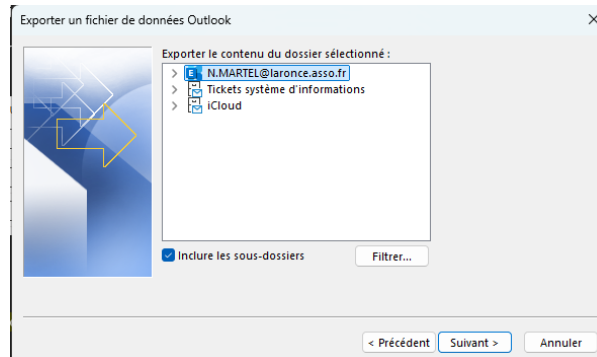
1)



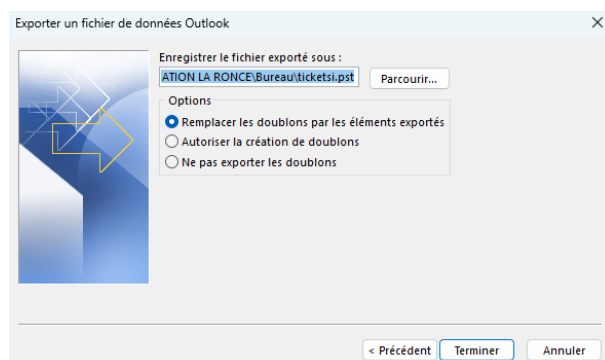
2)



3)



4)



Annexe n5

Script de création des nouveaux utilisateurs :

```
1 Add-Type -AssemblyName System.Windows.Forms
2 Add-Type -AssemblyName System.DirectoryServices.AccountManagement
3
4 # Créer le formulaire
5 $form = New-Object System.Windows.Forms.Form
6 $form.Text = "Création Utilisateur AD - La Ronce"
7 $form.Size = New-Object System.Drawing.Size(500, 400)
8 $form.StartPosition = "CenterScreen"
9
10 # Fonctions pour labels + textbox
11 function Add-LabelTextBox {
12     param (
13         [string]$LabelText,
14         [int]$top,
15         [ref]$textbox
16     )
17     $label = New-Object System.Windows.Forms.Label
18     $label.Text = $LabelText
19     $label.Left = 10
20     $label.Top = $top
21     $label.Width = 150
22     $form.Controls.Add($label)
23
24     $tb = New-Object System.Windows.Forms.TextBox
25     $tb.Left = 170
26     $tb.Top = $top
27     $tb.Width = 300
28     $form.Controls.Add($tb)
29     $textbox.Value = $tb
30 }
31
32 # UPN (dropdown)
33 $upnLabel = New-Object System.Windows.Forms.Label
34 $upnLabel.Text = "Domaine (UPN) :"
35 $upnLabel.Left = 10
36 $upnLabel.Top = 10
37 $form.Controls.Add($upnLabel)
38
39 $upnBox = New-Object System.Windows.Forms.ComboBox
40 $upnBox.Left = 170
41 $upnBox.Top = 10
42 $upnBox.Width = 300
43 $upnBox.Items.AddRange(@("laronce.asso.fr", "la-ronce.local"))
44 $upnBox.SelectedIndex = 0
45 $form.Controls.Add($upnBox)
46
47 $tbPrenom = $null
48 $tbNom = $null
49 $tbFonction = $null
50 $tbOU = $null
51
52 Add-LabelTextBox -LabelText "Prénom :" -top 40 -textbox ([ref]$tbPrenom)
53 Add-LabelTextBox -LabelText "Nom :" -top 70 -textbox ([ref]$tbNom)
54 Add-LabelTextBox -LabelText "Fonction :" -top 100 -textbox ([ref]$tbFonction)
55
56 # Choix de l'OU
57 $lbOU = New-Object System.Windows.Forms.Label
58 $lbOU.Text = "OU (Service) :"
59 $lbOU.Left = 10
60 $lbOU.Top = 130
61 $form.Controls.Add($lbOU)
62
63 $cbOU = New-Object System.Windows.Forms.ComboBox
64 $cbOU.Left = 170
65 $cbOU.Top = 130
66 $cbOU.Width = 300
67 $cbOU.DropDownStyle = "DropDownList"
68 $cbOU.Items.AddRange(@("CAMP",
69     "IMP",
70     "IMPRO",
71     "SAVS SAMSAH",
72     "SESSAD CL",
73     "SESSAD MC",
74     "SIEGE"
75 ))
76 $cbOU.SelectedIndex = 0
77 $form.Controls.Add($cbOU)
78
79 # Mot de passe
80 $lbPwd = New-Object System.Windows.Forms.Label
81 $lbPwd.Text = "Mot de passe :"
82 $lbPwd.Left = 10
83 $lbPwd.Top = 160
84 $form.Controls.Add($lbPwd)
85
86 $tbPwd = New-Object System.Windows.Forms.TextBox
87 $tbPwd.Left = 170
88 $tbPwd.Top = 160
89 $tbPwd.Width = 300
90 $tbPwd.UseSystemPasswordChar = $true
91 $form.Controls.Add($tbPwd)
92
93 $chkShowPwd = New-Object System.Windows.Forms.CheckBox
94 $chkShowPwd.Text = "Afficher le mot de passe"
95 $chkShowPwd.Left = 170
96 $chkShowPwd.Top = 190
```

```

99 $chkShowPwd.Add_CheckedChanged({
100     $tbPwd.UseSystemPasswordChar = -not $chkShowPwd.Checked
101 })
102 $form.Controls.Add($chkShowPwd)
103
104 # Bouton Création
105 $btnCreate = New-Object System.Windows.Forms.Button
106 $btnCreate.Text = "Créer Utilisateur"
107 $btnCreate.Left = 170
108 $btnCreate.Top = 230
109 $btnCreate.Width = 150
110 $form.Controls.Add($btnCreate)
111
112 # Résultat
113 $lblResult = New-Object System.Windows.Forms.Label
114 $lblResult.Left = 10
115 $lblResult.Top = 270
116 $lblResult.Width = 460
117 $lblResult.Height = 80
118 $lblResult.ForeColor = "DarkGreen"
119 $form.Controls.Add($lblResult)
120
121 # Action sur le bouton
122 $btnCreate.Add_Click({
123     try {
124         $prenom = $tbPrenom.Text.Trim()
125         $nom = $tbNom.Text.Trim()
126         $fonction = $tbFonction.Text.Trim()
127         $souName = $cbOU.SelectedItem
128         $mdp = $tbPwd.Text
129         $supn = $suprBox.SelectedItem
130
131         if (-not $prenom -or -not $nom -or -not $mdp -or -not $souName) {
132             [System.Windows.Forms.MessageBox]::Show("Tous les champs sont obligatoires !", "Erreur", "OK", "Error")
133             return
134         }
135
136         $sam = ($prenom.Substring(0,1) + "." + $nom).ToLower()
137         $email = ($prenom.Substring(0,1) + "." + $nom).ToLower() + "@laronce.asso.fr"
138         $userUPN = "$sam@$supn"
139         $ouDN = "OU=$souName,OU=Utilisateurs,DC=la-ronce,DC=local"
140
141         New-ADUser `
142             -SamAccountName $sam `
143             -UserPrincipalName $userUPN `
144             -Name "$prenom $nom" `
145             -GivenName $prenom `
146             -Surname $nom `
147             -DisplayName "$prenom $nom" `
148             -Title $fonction `
149             -Department $souName `
150             -Company "La Ronce" `
151             -EmailAddress $email `
152             -AccountPassword (ConvertTo-SecureString $mdp -AsPlainText -Force) `
153             -PasswordNeverExpires $true `
154             -CannotChangePassword $true `
155             -Enabled $true `
156             -Path $ouDN `
157             -OtherAttributes @{proxyAddresses = "SMTP:$email"}
158
159         Start-ADSyncSyncCycle -PolicyType Delta
160
161         $lblResult.Text = "✅ Utilisateur $prenom $nom créé avec succès ! nUPN: $userUPN nEmail: $email nproxyAddresses:SMTP:$email"
162     }
163     catch {
164         $lblResult.ForeColor = "DarkRed"
165         $lblResult.Text = "❌ Erreur : $($_.Exception.Message)"
166     }
167 })
168
169 # Affiche le formulaire
170 [void]$form.ShowDialog()
171

```

Annexe n6

Etapes réalisées au niveau de la sécurité

Action recommandée	Impact sur le score
Vérifier que le « partage externe » des calendriers n'est pas disponible	+0.48 %
Vérifier que les fournisseurs de stockage supplémentaires sont restreints dans Out	+0.48 %
Vérifier que tous les formulaires de transfert de courrier sont bloqués et/ou désacti	+0.48 %
Vérifier que les infos courrier sont activées pour les utilisateurs finaux	+0.29 %
Assurez-vous que la recherche du journal d'audit Microsoft 365 est activée	+0.29 %
Vérifier que l'audit de boîte aux lettres pour tous les utilisateurs est activé	+0.29 %
Vérifiez que les utilisateurs qui installent des compléments Outlook ne sont pas au	+0.29 %
Vérifiez que les stratégies de courrier indésirable Exchange Online sont définies po	+0.29 %
Seuls les utilisateurs invités doivent être automatiquement admis aux réunions Tea	+0.19 %
Configurer les utilisateurs autorisés à présenter dans les réunions Teams	+0.19 %
Déployer un collecteur de journaux pour découvrir l'activité d'informatique fantôm	+0.1 %
Restreindre l'accès des utilisateurs anonymes aux réunions	+0.1 %
Déconnecter les utilisateurs inactifs dans SharePoint Online	+0.1 %
S'assurer que l'authentification moderne pour les applications Microsoft Office Sha	+0.1 %
Bloquer les utilisateurs ayant atteint la limite de messages	+0.1 %
Créer des stratégies de liens fiables pour les courriers	+0.86 %
Activer les pièces jointes fiables en mode bloc	+0.76 %
Assurez-vous que l'intelligence de la boîte aux lettres est activée	+0.76 %
Assurez-vous que l'intelligence pour la protection contre l'usurpation d'identité est	+0.76 %
Déplacer les messages détectés comme utilisateurs usurpés par l'intelligence de la	+0.76 %
Activer la protection de domaine usurpé	+0.76 %
Définissez le seuil de niveau d'e-mail de phishing sur 2 ou plus	+0.76 %
Activer la protection des utilisateurs usurpés	+0.76 %
Créer des stratégies de vidage automatique de zéro heure pour les programmes ma	+0.57 %
Mettre en quarantaine les messages détectés à partir de domaines dont l'identité a	+0.57 %
Mettre en quarantaine les messages détectés provenant d'utilisateurs usurpés	+0.57 %
Activer Microsoft Defender pour Office 365 dans SharePoint, OneDrive et Microsoft T	+0.48 %
Activer les documents sécurisés pour les clients Office	+0.48 %
Vérifiez que le filtre des types de pièces jointes communs est activé	+0.48 %
Définir l'action à entreprendre en cas de détection de spam à haute fiabilité	+0.48 %
Définir l'action à entreprendre en cas de détection d'hameçonnage	+0.48 %
Définir l'action à entreprendre en cas de détection d'hameçonnage hautement fiabl	+0.48 %
Définir l'action à entreprendre en cas de détection de spam	+0.48 %
Vérifier que la stratégie pièces jointes fiables est activée	+0.48 %
Vérifiez que l'authentification moderne pour Exchange Online est activée	+0.29 %
Créer des stratégies de vidage automatique de zéro heure pour les messages d'han	+0.29 %
Définir l'action à entreprendre en cas de détection de spam en masse	+0.29 %
Activer le conseil de sécurité d'emprunt d'identité de domaine	+0.29 %
Activer le conseil de sécurité sur l'emprunt d'identité de l'utilisateur	+0.29 %

2	Activer l'astuce de sécurité relative à l'emprunt d'identité de l'utilisateur pour les ca	+0.29 %
3	Vérifier que les liens fiables pour les applications Office sont activés	+0.29 %
4	Vérifier qu'une stratégie anti-hameçonnage a été créée	+0.29 %
5	Assurez-vous qu'aucun domaine d'expéditeur n'est autorisé pour les stratégies ant	+0.19 %
3	Empêcher les utilisateurs connectés de contourner un hall de réunion	+0.1 %
3	Empêcher les participants externes d'avoir le contrôle d'une réunion Teams	+0.1 %
3	Empêcher les utilisateurs anonymes de démarrer des réunions Teams	+0.1 %
1	Ne pas ajouter d'adresses IP autorisées dans la politique de filtrage des connexion	+0.1 %
2	Créer des stratégies de vidage automatique de zéro heure pour les messages indés	+0.1 %
3	Conserver les spams en quarantaine pendant 30 jours	+0.1 %
4	Définissez le seuil du niveau de réclamation groupée (BCL) par e-mail sur 6 ou moi	+0.1 %
5	Définir les règles de transfert automatique des e-mails pour qu'elles soient contrôl	+0.1 %
5	Définir le nombre maximal de destinataires externes qu'un utilisateur peut envoyer	+0.1 %
7	Définir le nombre maximal de destinataires internes auxquels un utilisateur peut e	+0.1 %
3	Définir une limite quotidienne de messages	+0.1 %
1	Vérifier que l'authentification multifacteur est activée pour tous les utilisateurs	+0.86 %
3	Vérifiez que le consentement de l'utilisateur n'est pas accordé concernant l'accès	+0.38 %
2	Vérifiez que vous avez défini « Réinitialisation du mot de passe en libre-service acti	+0.1 %
3	Vérifier que l'authentification multifacteur est activée pour tous les utilisateurs aya	+0.96 %
5	Activer les stratégies d'accès conditionnel pour bloquer l'authentification héritée	+0.76 %
5	Vérifiez que la « Stratégie d'expiration du mot de passe » est définie sur « Définir les	+0.76 %
7	Vérifiez que la synchronisation du hachage du mot de passe est activée pour les dé	+0.48 %
5	Désignation de plusieurs administrateurs généraux	+0.1 %
7	Utiliser les rôles administratifs les moins privilégiés	+0.1 %

Annexe n7

Procédure pour débloquent l'enrôlement des postes dans Intune

Dans l'éditeur de registre :

*Ordinateur\HKEY_LOCAL
Microsoft \Enrollments*

MACHINE\SOFTWARE

Supprimer les clés différentes des autres

Dans l'explorateur de fichiers :

C:\Users\%username%\AppData\Local\Microsoft\identityCache

Supprimer le dossier 1

C:\Users\%username%\AppData\Local\Microsoft\OneAuth

Supprimer les dossiers *Accounts* et *Blobs*

Dans Paramètres :

Compte > Accès pro ou scolaire > déconnecter le compte Microsoft

Redémarrer le PC

Dans Word :

Connecter le compte de l'utilisateur et décocher la case "Laisser Microsoft gérer mon appareil"
sur la dernière fenêtre de connexion
Enfin cliquer sur "Oui toutes les applications"

Liste des acronymes

AD	Active Directory
ARS	Agence Régionale de Santé
BAL	Boîte aux lettres
CAMSP	Centre d'Action Médico-Sociale Précoce
CAF	Caisse d'Allocations Familiales
CRA	Centre de Rééducation Auditive
DDETS	Direction Départementale de l'Emploi, du Travail et des Solidarités
DSI	Directeur des Systèmes d'Information
GPO	Group Policy Object
IMPro	Institut Médico-Professionnel
IMP	Institut Médico-Pédagogique
MFA	Multi-Factor Authentication
OU	Organizational Unit (Unité d'Organisation)
POP	Post Office Protocol
SAMSAH	Service d'Accompagnement Médico-Social pour Adultes Handicapés
SAVS	Service d'Accompagnement à la Vie Sociale
SESSAD	Service d'Éducation Spéciale et de Soins à Domicile
SI	Systèmes d'Information
UPN	User Principal Name
XDR	Extended Detection and Response

Glossaire

Active Directory (AD) : Service d'annuaire centralisé de Microsoft, utilisé pour gérer les utilisateurs, ordinateurs, groupes et stratégies dans un réseau d'entreprise.

Azure AD / Entra ID : Version cloud d'Active Directory, utilisée dans les environnements Microsoft 365 pour gérer les identités et l'accès aux ressources.

Backup : Copie de sécurité des données permettant leur récupération en cas de suppression ou de panne.

Boîte aux lettres POP : Type de messagerie ancienne, stockant les mails uniquement en local sur le poste utilisateur, sans synchronisation ni sauvegarde serveur.

Boîte aux lettres IMAP : Messagerie moderne permettant la synchronisation des mails entre plusieurs appareils et le serveur.

Boîte collaborative (Zimbra) : Boîte mail avec fonctions collaboratives (calendrier partagé, partage de dossiers...), accessible via un client IMAP.

DNS (Domain Name System) : Système permettant de faire correspondre un nom de domaine (ex. la-ronce.fr) à une adresse IP.

Enrôlement hybride : Processus qui permet à un poste de faire partie à la fois de l'AD local et d'Entra ID/Intune pour un pilotage centralisé.

FIDO2 : Standard d'authentification physique sans mot de passe (clé USB sécurisée, etc.) renforçant la sécurité des accès.

GPO : Règle déployée via Active Directory pour appliquer automatiquement des paramètres (sécurité, raccourcis, mot de passe...) sur les postes du réseau.

Intune (Microsoft Endpoint Manager) : Solution de Microsoft permettant la gestion à distance des appareils (postes, tablettes, smartphones) via des stratégies de sécurité et de configuration.

Microsoft Defender XDR : Suite de sécurité Microsoft permettant la détection et réponse avancée aux menaces sur les postes, identités, mails, etc.

PowerShell : Interface en ligne de commande utilisée par les administrateurs pour automatiser des tâches comme la création de comptes ou la gestion des paramètres systèmes.

ProxyAddresses : Attribut AD permettant d'associer plusieurs adresses mail (alias) à un même utilisateur dans Exchange.

Synchronisation AD : Liaison entre l'AD local et Azure AD (via Azure AD Connect) permettant aux utilisateurs d'avoir le même compte/mot de passe local et cloud.